This Page is Inserted by IFW Indexing and Scanning Operations and is not part of the Official Record

BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- ☐ BLACK BORDERS
- ☐ IMAGE CUT OFF AT TOP, BOTTOM OR SIDES
- ☐ FADED TEXT OR DRAWING
- ☐ BLURRED OR ILLEGIBLE TEXT OR DRAWING
- ☐ SKEWED/SLANTED IMAGES
- ☐ COLOR OR BLACK AND WHITE PHOTOGRAPHS
- ☐ GRAY SCALE DOCUMENTS
- ☐ LINES OR MARKS ON ORIGINAL DOCUMENT
- ☐ REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY
- ☐ OTHER: _____

IMAGES ARE BEST AVAILABLE COPY.
As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/800,346	03/05/2001	Brian Manahan	155638-0037	3044

1622 7590 09/08/2004

IRELL & MANELLA LLP
840 NEWPORT CENTER DRIVE
SUITE 400
NEWPORT BEACH, CA 92660

EXAMINER	
HUA, LY	

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 09/08/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/800,346	MANAHAN, BRIAN
	Examiner	Art Unit
	Ly V. Hua	2135

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-24* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-24* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

   A person shall be entitled to a patent unless –

   .(a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

2. Claims 1, 8, 15 and 21, claims 5 and 11 claims 2, 9 and 16, claims 6, 12, 19 and 22, claims 7, 20 and 23 are rejected under 35 U.S.C. 102(a) as being anticipated by Yoshiura et al (6,131,162 hereinafter Yoshiura).

3. The following table lists the independent claims in parallel for ease of inspection.

4. .1. A method, comprising:	5. .15. A method, comprising:	6. .8. A computer system, comprising:	7. .21. A method, comprising:
a. digitally signing i with a private key ii to provide a digital signature; iii a web page that includes **a trigger;** b. transmitting i the web page**[that include the trigger]**, ii the digital signature, and iii a digital certificate iv from **a first computer system** v to ***a second computer system***; and **c. responsive to the trigger,** i automatically verifying (1) the digital signature (2) on the second computer system (3) using a public key corresponding to the private key.	a. receiving i a request for a web page; b. digitally signing i with a private key, ii to provide a digital signature, iii the web page that includes a trigger; c. transmitting i the web page **[that include the trigger]**, ii the digital signature, and iii a digital certificate iv to the computer system v in response to receiving the request for the web page; d. [wherein] i said trigger (1) for causing a program on a computer system (2) to automatically verify (a) the digital signature of the web page; and	a. a memory including one or more instructions; and b. a processor coupled to the memory, the processor, i responsive to the one or more instructions, to, (1) transmit (a) a request for a web page (b) over a communication link, (2) receive (a) **the web page including** (i) **a trigger,** (ii) a digital signature, and (iii) a digital certificate, and **ii responsive to the trigger,** (1) automatically verify (a) the digital signature of the web page (b) using a public key corresponding to a private key used to digitally sign the web page.	a. transmitting i a web page that includes a trigger ii from ***a first computer system*** iii to **a second computer system;** *b.* displaying *i* the web page *ii* on a display of **the second computer system;** c. detecting i the trigger ii by a program executed on a processor of **the second computer system;** d. automatically requesting that i the web page be digitally signed; e. digitally signing i the web page ii with a private key iii to provide a digital signature; and f. transmitting i the web page, ii digital signature, and iii a digital certificate iv to ***the first computer system***.

g. As to claim 1:

i Claim 1 claims:

(1) 1. A method comprising:

(a) digitally signing
(i) with a private key
(ii) to provide a digital signature;
(iii) a web page
1) that includes
a) **a trigger**

(b) transmitting
(i) the web page[**that include the trigger**],
(ii) the digital signature, and
(iii) a digital certificate
(iv) from **a first computer system**
(v) to ***a second computer system***; and

(c) responsive to the trigger,
(i) automatically verifying
1) the digital signature
2) on the second computer system
3) using a public key corresponding to the private key.

ii Yoshiura et al (6,131,162 herein after Yoshuira) teaches [see Detailed Description Text – DETX (172), (218)]:

(1) digitally signing
(a) a web page
(i) the includes
1) a trigger [i.e., a mark],
(b) to provide/[create]
(i) a digital signature [i.e., the digital signature contained in the mark],
(2) transmitting
(a) the web page,
(b) the digital signature [contained in the mark]
(c) from a first computer system
(d) to a second computer system; and
(3) responsive to the trigger/[mark]
(a) verifying
(i) the digital signature
(ii) on the second computer system
(iii) using a key corresponding to a key used to generate the digital signature.

h. As to claims 8, 15 and 21:

i These claims have limitations that are similar to those of claim 1. These claims are thus similarly rejected with the same rationales applied against claim 1.

i. As claims 5 and 11:
   i These claims claim:

   (1) .5. The method of claim 1 wherein
      (a) digitally signing comprises:
         (i) hashing the web page to provide a message digest; and
         (ii) digitally signing the message digest with a private key to provide the digital signature.

   (2) .11. The apparatus of claim 8 wherein the processor
      (a) automatically verifies
         (i) the digital signature of the web page
         (ii) by
            1) hashing the web page to provide a calculated message digest;
            2) decrypting the digital signature using the public key to provide a recovered message digest; and
            3) comparing the calculated message digest and the recovered message digest.

   ii Yoshiura teaches:

   (1) digitally signing a web-page, which signing comprising:
      (a) hashing
         (i) the web page
         (ii) to provide
            1) a message digest/[hash value]; and
      (b) digitally signing/[encrypting]
         (i) the message digest /[hash value]
         (ii) with a private key to
         (iii) provide the digital signature,
   (2) in that Yoshiura teaches the following:
      (a) [Detailed Description Text - DETX (211)]:
         (i) "That is, the server 1810a calculates a hash value 2807 of Web page data 2806 sent with the mark-send request (step 2801), encrypts the hash value 2807 with a private key 2808 of the mark management organization 1121 to generate a digital signature 2809 (step 2802), and embeds the generated digital signature 2809 into a mark 2810, stored in the mark management DB 1123, as a digital watermark (step 2803). The server 1810a then modifies the Web page data 2806 sent with the mark-send request so that a mark 2811 into which the digital watermark was embedded is displayed in the Web page 2806 (step 2804), and sends modified Web page data 2812 to the mark acquisition program e 3306 running on the vendor terminal 1112a (step 2805)"; and
      (b) [Detailed Description Text - DETX (218)]:
         (i) "In the eighth embodiment described above, a mark in which a digital signature, generated by encrypting the hash value of a Web page using the private key of the mark management organization mark, is embedded as a digital watermark and is pasted in a Web page instead of a simple mark. This type of mark enables the authentication of the relation between the Web page and the mark management organization to be validated correctly. The Web page also contains a mark showing the related individual/organization. In addition, because the digital signature for the hash value of the Web page data is always embedded into the mark as the digital watermark, the processing does not depend on whether a plurality of types of data are included in the Web page. Embedding the digital watermark into the mark in the Web page as the digital signature eliminates the need to manage the digital signature separately from the Web page data. Because the mark, usually displayed in the Web page, is used to authenticate

that the mark is given to the Web page, the eighth embodiment does not affect the appearance of the Web page".

iii Yoshiura teaches:

(1) verifying the digital signature of the web-page by:
  (a) hashing [step 2904]
    (i) the web page
    (ii) to provide
      1) a calculated message digest;
  (b) decrypting [step 2904]
    (i) the digital signature
    (ii) using the public key
    (iii) to provide
      1) a recovered message digest; and
  (c) comparing [step 2905]
    (i) the calculated message digest and
    (ii) the recovered message digest,

(2) in that Yoshiura teaches the following:
  (a) [Brief Summary Text - BSTX (16)]:
    (i) "In this case, the digital signatures created by n signature creators are verified as follows. The final digital signature is decrypted by the public key of the final (n-th) signature creator, the decrypted digital signature is then decrypted by the public key of the (n-1)th signature creator, and so on, until the digital signature of the first signature creator is decrypted. If the result obtained by decrypting the signature by the public key of the first signature creator matches the hash value of the original data, it is determined that the digital signature was created by n signature creators each having his or her own public key and that the digital signature corresponds to the data. However, when the sequence in which the signature creators created signatures is not known, this technique requires that the above process be performed for the number of times generated by permutating all signature creators."

j. As per claims 2, 16 and 9:

i These claims claim:

(1) .2. The method of claim 1 wherein
  (a) transmitting comprises transmitting
    (i) the web page,
    (ii) the digital signature, and
    (iii) the digital certificate including
      1) the public key corresponding to the private key
    (iv) from the first computer system
    (v) to the second computer system.

(2) .16. The method of claim 15 wherein
  (a) transmitting comprises transmitting
    (i) the web page,
    (ii) the digital signature, and
      1) the digital certificate including
        a) a public key corresponding to the private key
    (iii) to the computer system,

(iv) in response to receiving the request for the web page.

(3) .9. The apparatus of claim 8 wherein
(a) the processor,
(i) in response to the one or more instructions,
(ii) to receive
1) the web page,
2) digital signature, and
3) the digital certificate
a) including the public key.

ii **Yoshiura ('162)** teaches [Brief Summary Text - BSTX (8), (13), (16), (32), (56), (58), (66), (69), (72), (73) and (74)]:
(1) transmitting
(a) a web-page,
(b) a digital signature; and
(c) the public key
(d) form the first computer
(e) to the second computer.

k. As to claims 6, 19, 12, and 22:
i These claims claim:
(1) .6. The method of claim 1 wherein **the trigger includes**
(a) **one or more of the following**:
(i) a flag,
(ii) variable,
(iii) one or more lines of code, and
(iv) subroutine.
(2) .19. The method of claim 15 wherein **the trigger includes**
(a) one or more of the following:
(i) a flag,
(ii) variable,
(iii) one or more lines of code, and
(iv) subroutine.
(3) .12. The apparatus of claim 8 wherein the trigger includes
(a) one or more of the following:
(i) a flag,
(ii) variable,
(iii) one or more lines of code, and
(iv) subroutine.
(4) .22. The method of claim 21 wherein the trigger includes
(a) one or more of the following:
(i) a flag,
(ii) variable,
(iii) one or more lines of code, and
(iv) subroutine.
ii **Yoshiura ('162)** teaches:
(1) that the trigger/[mark] include
(a) flag/[a water mark].

l. As to claims 7, 20 and 23:
   i These claims claim:

      (1) .7. The method of claim 1 further comprising one of the following:
         (a) embedding the trigger in the web page;
         (b) incorporating the trigger in the web page;
         (c) appending the trigger to the web page; and
         (d) placing the trigger in a HTTP header of the web page.

      (2) .20. The method of claim 15 further comprising one of the following:
         (a) embedding the trigger in the web page;
         (b) incorporating the trigger in the web page;
         (c) appending the trigger to the web page; and
         (d) placing the trigger in a HTTP header of the web page.

      (3) .23. The method of claim 21 further comprising one of the following:
         (a) embedding the trigger in the web page;
         (b) incorporating the trigger in the web page;
         (c) appending the trigger to the web page; and
         (d) placing the trigger in a HTTP header of the web page.

   ii Yoshiura ('162) teaches [see Detailed Description Text 0 DETX (218); Claims Text – CLTX (152), 174]:
      (1) embedding/incorporating/appending/"generating and embedding"
         (a) a trigger [mark/information for checking the validity of a Web page]
         (b) into a web-page.

Claim Rejections - 35 USC § 103

1. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

.(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

2. Claim 3, 4, 17, 18 and 10 are rejected under 35 U.S.C. 103(a) as being obvious over Yoshiura et al (6,131,162 hereinafter Yoshiura) as applied to claims 1, 8, 15 and 21 above, and further in view of either common practice in the art of Aieta et al. (6,269,349 hereinafter Aieta).

m. As to claims 3, 4, 17, 18 and 10:
   i These claims claims:

      (1) .3. The method of claim 1 wherein transmitting comprises transmitting
         (a) the web page,
         (b) the digital signature,
         (c) the digital certificate, and
         (d) an object
         (e) from the first computer system

(f) to the second computer system.

(2) .4. The method of claim 3 wherein automatically verifying comprises
(a) responsive to the trigger,
(i) automatically verifying
1) the digital signature
2) on the second computer system
3) using the object.

(3) .17. The method of claim 15 wherein transmitting comprises transmitting
(a) the web page,
(b) the digital signature,
(c) the digital certificate, and
(d) an object
(e) to the computer system,
(f) in response to receiving the request for the web page.

(4) .18. The method of claim 17 wherein
(a) said object, on the computer system,
(i) for detecting the trigger, and
(ii) in response to detecting the trigger,
1) automatically verifying
a) the digital signature of the web page.

(5) .10. The apparatus of claim 8 wherein the processor, in response to the one or more instructions, to receive
(a) the web page,
(b) digital signature,
(c) digital certificate, and
(d) an object,
(i) said object being executed
1) by the processor
2) to automatically verify the digital signature of the web page.

ii **Official notice is hereby taken** that:
(1) transmitting
(a) an executable object
(i) along with information,
1) which is to be processed
a) by the executable object,
(ii) to a receiver/destination
(b) is notoriously old and well known in the art.

iii **Aieta et al (6,269,349 hereinafter Aieta)** teaches [see Claims Text - CLTX (38), CLTX (65)]:
(1) transmitting an executable object to the client; and
(2) 27. The system of claim 17, wherein when receiving the private information, the processor is further configured to transmit an executable object to the client and receive the private information from the object after the object is activated at the client.

iv It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:
(1) apply the concept of sending an executable object from transmitting node to receiving node as that of Aieta to have the receiving node executes a procedure according the instructions of the executable object.

v The skilled person would have been motivated to upload (optionally) an executable object to a receiving node (such as that of Yoshiura) to have the receiving node executes the executable object to perform the function thereat because:
(1) it is a common practice in the art, especially when it is aware by the transmitting node that receiving node might not have the executable object; and
(2) Aieta teach the usage of such executable object, which is sent by a transmitting node and executed by a receiving node.

3. Claim 13, 14 and 24 are rejected under 35 U.S.C. 103(a) as being obvious over Yoshiura et al (6,131,162 hereinafter Yoshiura) as applied to claims 1, 8, 15 and 21 above, and further in view of common practice in the art.

n. As to claims 13, 14 and 24:
i These claims claim:
(1) .13. The apparatus of claim 8 wherein the memory includes
(a) a software routine
(i) for plug-in comprising the one or more instructions.

(2) .14. The apparatus of claim 8 wherein the memory includes
(a) one of
(i) a browser software program and
(ii) a plug-in comprising the one or more instructions.

(3) .24. The method of claim 21 wherein
(a) the program is one or more of the following:
(i) a plug in and
(ii) browser program.

ii Official notice is hereby taken that:
(1) memory [such as CD, DVD, memory-card, smart-card],
(a) which include instruction code [plug-in instruction code]
(i) for causing
1) a computer
a) (into which it is plugged)
b) to request
i) web page(s) from a server/[source]/[provider]/[vendor]/[provider of the memory],
(b) is notoriously old and well known in the art.
(2) [An example of such well known feature is American Online promotional storage medium that are sent to people so that they can load into their computer for downloading AOL web pages for subscribing service from AOL server(s)].

iii It would have been obvious to a person having ordinary skill in the art at the time the invention was made to:
(1) apply the teaching of Yoshiura ('162) to a web page that is downloaded from a well known plug-in instruction.

iv The skilled person would have been motivated to do such application because:
(1) the teaching of Yoshiura is to authenticate that the web-page is coming from an authentic web-page provider; and
(2) Internet browser (such as that of American Online) download web-page(s) from web-page provider(s).

8. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ly V. Hua whose telephone number is (703) 305-9684. The examiner can normally be reached on Monday to Friday from 9:00 AM to 5:30 PM.

   If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Vu Kim, can be reached on 703-305-4303. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

   Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ly V. Hua
Primary Examiner
Art Unit 2135

Lvh
August 9, 2004